CREST
CPIA
CREST Practitioner Intrusion Analyst (CPIA)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

Endpoint protection on a design workstation quarantines plotsvc.exe as Heur.Suspicious.Gen. A multi-engine scanning service reports 2 of 68 engines flagging the file, both with generic heuristic names. The file carries a valid signature from the plotter manufacturer, and its hash appears in a known-good software reference set.
What is the best assessment?

A. A likely false positive, to be confirmed and reported
B. A confirmed infection that needs immediate eradication on the host
C. Evidence the file executed on this host
D. Targeted malware evading most engines, given the low detection count
E. A false positive best resolved by disabling the heuristic engine everywhere

Answer: A

Question: 2

Across an estate of 4,000 hosts, an analyst summarises a week of proxy data for five external destinations:
av-update.example.com: all 4,000 hosts, hourly, day and night
files.example.org: one host, irregular large downloads, office hours only
share.example.net: one host, a single 2 GB upload
img-cache.example.net: two hosts, every 15 minutes with slight jitter, about 1 KB each, day and night
calendar.example.org: 3,200 hosts, every 5 minutes, office hours only
Which destination is the strongest beacon candidate?

A. av-update.example.com, contacted hourly by every host
B. files.example.org, with irregular large downloads
C. img-cache.example.net, contacted by two hosts around the clock
D. share.example.net, after its single large upload
E. calendar.example.org, polled every five minutes by most hosts in office hours

Answer: C

Question: 3

Packet captures from a two-week monitoring deployment may be relied on in disciplinary proceedings. The analyst reviews the handling record for the capture files.

Which entry most weakens the evidential integrity of the captures?

A. Analysis was performed on working copies of the capture files
B. The sensor clock was synchronised to the internal NTP source
C. Capture files were rotated into 1 GB segments during collection
D. Original segment files were written to write-once media at the end of collection
E. Files were first hashed after being copied onto the analyst's laptop

Answer: E

Question: 4

Threat intelligence on a malware family states that its implant beacons over HTTPS with a base interval of ten minutes and up to 30% random jitter, changes its URI path on every request, and keeps each check-in under 2 KB.
Which detection approach is most likely to surface infected hosts in proxy logs?

A. Alert on any host contacting one destination at an exact ten-minute interval
B. Write a signature for the URI path seen in the published sample
C. Flag the hosts with the highest total outbound byte counts each day
D. Model the spread of intervals for every host-destination pair
E. Search for DNS NXDOMAIN bursts from each host

Answer: D

Question: 5

Before an engagement, an analyst is building a picture of a logistics client's internal technology from open sources only, without touching any of the client's systems.
Which source is most likely to reveal the specific firewall and endpoint products the client runs?

A. The client's domain WHOIS record
B. Job adverts and staff profiles on professional networks
C. The IP WHOIS allocation for the client's public address range
D. An active Nmap service scan of the client's internet perimeter
E. Sector threat reports from antivirus vendors

Answer: B

Question: 6

While investigating a compromised e-commerce web server for an online retailer, the analyst finds a script that has copied cardholder names, card numbers and expiry dates to 203.0.113.77 for three weeks. The engagement is for technical analysis only.
What is the analyst's most appropriate action regarding notification?

A. Notify the card brands directly so the affected cards can be blocked
B. Report the exfiltration to the police before informing the client
C. Hold the finding back until the root cause is fully confirmed
D. Ask the national CERT for a takedown
E. Report it promptly to the client and its counsel

Answer: E

Question: 7

During a privilege-escalation review of a Windows workstation, an analyst exports the ACLs of several registry keys. The service ScanAgent runs as LocalSystem.
Which finding presents the greatest risk of a standard user gaining SYSTEM privileges?

A. BUILTIN\Users hold Read on HKLM\SYSTEM\CurrentControlSet\Services
B. BUILTIN\Users hold Set Value on the HKLM\SYSTEM\CurrentControlSet\Services\ScanAgent key
C. Each user holds Full Control over their own HKCU\Software\Microsoft\Windows\CurrentVersion\Run key
D. BUILTIN\Administrators hold Full Control on HKLM\SOFTWARE
E. SYSTEM holds Full Control on HKLM\SAM

Answer: B

Question: 8

Investigating a charity's finance PC, an analyst finds that HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run has a last-write time of 2026-08-11 02:14 UTC. The key holds four values: three vendor updaters and one unknown value, svcupd. A colleague's draft states that svcupd was added at 02:14.
How should that statement be evaluated?

A. Proven, as each value carries its own creation time matching the key's last-write time
B. Proven, as a key's last-write time changes only when a new value is added to it
C. Unproven, as the key time shows only when the hive was last loaded at boot
D. Unproven: values carry no timestamp
E. Proven for whichever value is listed last, as values are stored in the order added

Answer: D

Question: 9

Reverse engineering of a ransomware sample shows that it encrypts each file with a random AES key, then encrypts that AES key with an RSA public key embedded in the binary and stores the result in the file trailer. A manager asks whether the extracted public key can be used to restore the files.
What is the best answer?

A. No; it only encrypts, and decrypting the AES keys needs the private key
B. Yes; the key that encrypted the AES keys can also decrypt them
C. Yes, once it has been converted into a matching AES key of the same bit length
D. No; the files were protected by RC4, and AES played no part
E. Yes, if it is combined with each file's MD5 hash

Answer: A

Question: 10

An analyst at a water utility runs a suspected loader on an analysis VM with its network adapter disconnected. Process and packet monitoring show the sample start, attempt to resolve update-check.example.org, receive a lookup failure and exit after four seconds. No files, registry values or child processes are created. Static triage found no debugger checks, VM-artefact strings or long sleeps.
What is the best next step in the live analysis?

A. Connect the VM directly to the internet and let the sample reach its server
B. Record it as benign, with no file, registry or process change seen at all
C. Re-run it on a host-only network with fake DNS and fake HTTP services
D. Stop live work and rely on disassembly of the sample alone
E. Run it on a spare production workstation with normal internet access

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/